



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/588,879

08/09/2006

George E. Hoffman

4003.PALM.PSI

4106

49637 7590 04/09/2012  
BERRY & ASSOCIATES P.C.  
9229 SUNSET BOULEVARD  
SUITE 630  
LOS ANGELES, CA 90069

EXAMINER

LEE, CHUN KUAN

ART UNIT

PAPER NUMBER

2181

NOTIFICATION DATE

DELIVERY MODE

04/09/2012

ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

efiling@berrypc.com

<b>Office Action Summary</b>	<b>Application No.</b> 10/588,879	<b>Applicant(s)</b> HOFFMAN ET AL.	
	<b>Examiner</b> Chun-Kuan Lee	<b>Art Unit</b> 2181	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 17 February 2012.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 5) ☒ Claim(s) 1,4-21 and 31-40 is/are pending in the application.
- 5a) Of the above claim(s) 32-40 is/are withdrawn from consideration.
- 6) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 7) ☒ Claim(s) 1,4-21 and 31 is/are rejected.
- 8) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 9) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☒ The drawing(s) filed on 09 August 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 12) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                       | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. ____.                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>09/07/2011</u> .  | 6) <input type="checkbox"/> Other: ____.                          |

## DETAILED ACTION

### RESPONSE TO ARGUMENTS

1. Applicant's arguments filed 07/25/2011 have been fully considered but they are not persuasive. Currently, claims 32-40 are withdrawn, and claims 1, 4-21 and 31 are pending for examination.

2. In response to applicant's arguments with regard to the independent claims 1, 20-21 and 31 rejected under 35 U.S.C. 103(a) that Scheifler and Colburn are being read too broadly, wherein analysis of whether Scheifler utilizes a centralized authority must be conducted outside that of a keyword search of the reference, as Scheifler is limited to what it discloses in its drawings, specification, and claims; furthermore, if the only embodiment disclosed is the exemplary embodiment, then Scheifler's disclosure cannot be expanded to structures or contexts outside of its disclosure; additionally, Scheifler's claim 1 further supports Applicants' view and that there are no other implementations disclosed, wherein claim 1 states in part:

A system that regulates access to a resource requested by an operation executing on a computer, the operation invoking a plurality of functions that operate upon code during execution, the system comprising:

a policy file that stores permissions for each of the functions, the permissions authorizing types of access to the resource based on a source of the code and the executor of the code. Col. 21, lines 15-22.

again, without using the term centralized, Scheifler has disclosed a centralized scheme; there is no other indication that the security policy for a resource is set any other way; Scheifler explicitly requires a security policy file, which by definition is a

Art Unit: 2181

centralized location for setting security policy, because Scheifler has not disclosed any other structure, it is limited to the structure it does disclose; therefore, Applicants' respectfully submit Scheifler is being expanding beyond its capabilities and outside the context of a centralized scheme; applicant's arguments have fully been considered, but are not found to be persuasive.

The examiner respectfully disagrees; and to further clarify the examiner's position, as indicated in applicant's remarks, Scheifler's claim 1 does not claim a "centralized policy file" or "central policy file" (i.e. policy file in Scheifler's claim 1 is recited "without using the term centralized"); therefore, Scheifler's claimed invention do not limit "policy file" to a specific locality; additionally, in association with applicant's citation of Scheifler's claim 1, Scheifler does indicate that various alternatives are possible and that the exemplary embodiments are not intended to limit the claimed invention to the precise form disclosed:

"... While one method of tracking which invocations are enabling invocations is described above, various alternative methods of tracking enabling invocations are possible. Therefore, it is understood that the present invention is not limited to any specific method for tracking enabling invocations.

#### CONCLUSION

Systems and methods consistent with the principles of the present invention provide a security enforcement mechanism in which access permissions of a thread vary over time based on the source and executor of the code being executed.

The foregoing description of exemplary embodiments of the present invention provides illustration and description, but is not intended to be exhaustive or to limit the invention to the precise form disclosed. Modifications and variations are possible in light of the above teachings or may be acquired from practice of the invention. The scope of the invention is defined by the claims and their equivalents.

Although systems and methods consistent with the present invention are described as operating in the exemplary distributed system and the Java programming environment, one skilled in the art will appreciate that the present invention can be practiced in other systems and other programming environments. Additionally, although aspects of the present invention are described as being stored in memory, one skilled in

Art Unit: 2181

the art will appreciate that these aspects can also be stored on or read from other types of computer-readable media, such as secondary storage devices, like hard disks, floppy disks, or CD-ROM; a carrier wave from the Internet; or other forms of RAM or ROM. Sun, Sun Microsystems, the Sun logo, Java, and Java-based trademarks are trademarks or registered trademarks of Sun Microsystems Inc. in the United States and other countries ...” (Scheifler, col. 20, l. 46 to co.. 21, l. 13)

Therefore, Scheifler’s exemplary embodiment is not intend to limit Scheifler’s claimed invention as it is an example on how Scheifler’s claimed invention may be implemented. In summary, applicant’s analysis of Scheifler’s claimed invention appears to be more limiting then Scheifler’s actual claimed limitations, wherein Scheifler does not limit Scheifler’s “policy file” to be centralized.

3. In response to applicant’s arguments with regard to the independent claims 1, 20-21 and 31 rejected under 35 U.S.C. 103(a) that the examiner states that he is relying on the combined teachings to teach security permissions are not granted based on a call to a first interface; assuming this is not a mistake, the examiner has proved the Applicants' case; applicant's arguments have fully been considered, but are not found to be persuasive.

The examiner respectfully disagrees; and based on the examiner’s extensive explanation during the prosecution and the preceding office action’s rejected claims and examiner’s remarks, the examiner clearly intended to indicate that the combined teachings to teach security permissions are granted, rather than not granted.

4. In response to applicant’s arguments with regard to the independent claims 1, 20-21 and 31 rejected under 35 U.S.C. 103(a) that the combination of the references

Art Unit: 2181

does not teach/suggest every claimed features because Scheifler and Colburn are being read too broadly as:

- Scheifler is directed towards a security approach that utilizes a centralized security policy file to store permissions for a particular resource, and support for "centralized" security policy file are as following:
  - Figure 4, is a representation of Scheifler's system that exemplifies a "centralized" security scheme; security (e.g., permissions) is stored in a policy file (Fig. 4, ref. 4100); this policy file is the centralized storage for the various permissions available within the resource (though the word "centralized" is not used, the structure of Scheifler when properly examined reveals the centralized structure); each permission, executor, resource, and capability are represented in this file (See e.g., Fig. 5, which stores permissions for Executor 1 to Executor N.)
  - the security mechanism of a system in Scheifler uses "permission objects and protection domain objects to store information that models the security policy of the system." Col. 8, lines 24-27;
  - a protection domain is "a set of permissions granted to one or more executors when code from one or more sources is being executed on their behalf." Col. 11, lines 23-26;
  - as shown in Fig. 4, the protection domain object (ref. 4400) is external to object (ref. 4500);

- a permission object may also represent permissions of a system; permission objects derive permissions from the policy file (ref. 4100) for a given system. See Fig. 4; the permission object contains the methods for determining permissions of other objects. Col. 11, lines 54-56;
- any security permission and access (whether implied or explicit) is validated using a method within a permission object. See e.g., col. 12, lines 46-55;
- to implement the security policy of the system, a policy object, domain mapper object, one or more protection domain objects, and one or more access identifiers are needed. Col. 12, lines 61-65 and Fig. 4; Scheifler outlines the centralized structure of the system Col. 12, line 66 - col. 13, line 6; and
- Schiefler stores security policy that is centrally designated by a policy file in a policy object; this policy object is external to an object that may utilize its security validation methods; and
- permissions in Scheifler are not determined at an interface of the target object as presently claimed, and by consulting a protection domain object that derives its permissions from a policy file that is centralized with respect to the policy objects, domains, and executing objects;

Colburn's sole disclosure is "FIG. 8 is a block diagram illustrating target constraints 184 associated with target object 160." (Col. 10, lines 52-53), and from that,

Art Unit: 2181

the examiner leaps to stating that the security policy of a target object is contained solely within the target object; the examiner must ignore the rest of Colburn's teaching;

Colburn does not grant security permission examining a security policy contained entirely within the target object and solely determined by the first interface; access is granted based on a combination of owner identifier and access authorizations; the access authorizations are not interface based but arbitrary designations that enable different levels of access to the objects; the access is not granted to other interface according the determination as claimed; rather access is granted based on the interface designation; if the interface has the improper designation, no other access to other interfaces of the object is granted;

Colburn discloses authorization that creator/owner must implement into their objects, and requires identification of the entity that creates an object definition and access is granted with regard to the computer system (i.e. security permissions are not granted based on a call to a first interface and the security policy of a target object is certainly not contained solely within the target object as claimed); and Colburn's access authorizations are not interface based but arbitrary designations that enable different levels of access to the objects, and in order for the access to be resolved the owner identifier must be resolved, which necessarily involves a process outside of a particular object (col. 14, lines 5-13); moreover, Colburn's discussion of dynamic inheritance is further evidence that security is not determined as claimed (e.g., Fig. 11 and corresponding description col. 14, line 35 - col. 16, line 21); applicant's arguments have fully been considered, but are not found to be persuasive.

The examiner respectfully disagrees; first of all, in all of applicant's citations with regard to Scheifler's disclosure, Scheifler's did not either expressly utilized the term "centralized" or a term that is synonymous to "centralized;" therefore, Scheifler's invention is not limited to or require a "centralized" security policy file; and if the "centralized" security policy file was an essential requirement to implementing Scheifler's invention, Scheifler would certainly have expressly include the term or synonymous term of "centralized"; additionally, applicant's current argument with regarding to Scheifler having "centralized" security policy file is based on applicant's interpretation of Scheifler's figure/structure without Scheifler's specification expressly disclosing the "centralized" requirement; and even if applicant's interpretation of Scheifler's was accurate, Scheifler's "centralized" security policy file is an exemplary implementation of Scheifler's invention, not a limiting requirement; more specifically, Scheifler does disclose the utilization of the security policy file, but does not require/limit the architecture/structure associated with the security policy file as being "centralized". Additionally, the examiner is relying on Scheifler, not Colburn, for the teaching/suggestion with regard to interface based access authorization.

Colburn does teach/suggest the security policy (Fig. 8, ref. 194, 194) of a target object (Fig. 8, ref. 160) is contained solely within the target object (Fig. 8); and the examiner is relying on the combined teaching of Scheifler and Colburn for the teaching/suggestion of security permissions are granted based on a call to a first interface, not relying on Colburn along; and with regard to Colburn's disclosure in col. 14, lines 5-13, Colburn indicated that the "... access is permitted through the target ...,"

Art Unit: 2181

wherein the server, where the target is located, implements secure accessing in association with the user requesting access having appropriate access authorization; therefore, the secure accessing being implemented by the server having the target object do not involve a process outside a particular object; lastly, assuming the applicant's analysis of Colburn is accurate, the examiner is not fully clear as to how Colburn's discussion of dynamic inheritance is evidence that security is not determined as claimed; therefore, the examiner is unable to properly address applicant's arguments. Additionally, the examiner is not ignoring Colburn's teaching as a whole, Colburn's Figure 8 does teach/suggest that the security policy (Fig. 8, ref. 194, 194) of a target object (Fig. 8, ref. 160) is contained solely within the target object (Fig. 8), as security permission is granted in associated with the target implementing the determination based on the target receiving the owner's identifier and the target's security policy (i.e. whether to grant access or not is determined at the target).

Additionally, please note that one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

5. In response to applicant's arguments that because both Scheifler and the present invention may utilize object oriented programming is an improper reason for rendering the claims obvious or combining two references as Scheifler's system and method present a differing structure and functionality that is distinguishable from the presently

Art Unit: 2181

claimed invention; wherein applicant's arguments appear to indicate that Scheifler is non-analogous art; applicant's arguments have fully been considered, but are not found to be persuasive.

Please note that it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Scheifler is in the field of applicant's endeavor as Scheifler discloses implementing security measures associated with object oriented programming; more specifically, Scheifler is not just disclosing object oriented programming, but Scheifler also disclose the implementation of security measures.

As applicant appears to be applying the above arguments towards independent claims 1, 20-21 and 31, the examiner will also apply the above responses toward independent claims 1, 20-21 and 31.

6. In response to applicant's arguments with regard to the independent claims 1, 20-21 and 31 rejected under 35 U.S.C. 103(a) that the Scheifler-Colburn combination is improper because combining Colburn with Scheifler impermissibly changes the principle operation of Scheifler as Scheifler stores security details (e.g., permissions) in a centralized policy file not in target objects as claimed (e.g., Figure 4) and Colburn relies on an owner-identifier being incorporated into objects; this identifier is based on the creator of an object or the system used to create the object; so that Colburn's system

Art Unit: 2181

may function, Colburn defines a set of access authorizations that creators must implement into their objects (See col. 9, Table 1), Attribute Name Access Authorization (Applicants believe this table along with the associated discussion below the table, col. 9, lines 21-41, outlines the definitions of the set of access authorization clearly enough so that the examiner may "properly respond to applicant's arguments."); Colburn's system is not based on a centralized authority controlling security details, but the existence of an owner identifier and a standardized system of access authorizations (e.g., Abstract, col. 8, line 60 - col. 9, line 41, and col. 10, lines 6 – 51); therefore, combination of Colburn with Scheifler requires abandoning Scheifler's use of a centralized authority (e.g., the policy file) to determine security; and conversely, incorporating Scheifler into Colburn requires Colburn to adopt Scheifler's use of centralized permission objects; both systems describe two different specific implementations of controlling access that are not compatible; for this reason alone, the combination is improper and the prima facie case of obviousness has not been met; applicant's arguments have fully been considered, but are not found to be persuasive.

The examiner respectfully disagrees, as discussed in detail above, Scheifler's use of a centralized authority is based on applicant's interpretation without Scheifler's specification expressly disclosing such requirement, and even if applicant's interpretation were accurate, Scheifler's use of centralized authority is an exemplary implementing of Scheifler's invention, not a limiting requirement. Therefore, it would not be improper to combine the Colburn with Scheifler, as the resulting combination of the

Art Unit: 2181

references teaches/suggests the determination associated with the security proceedings being implemented at the target.

Furthermore, as explained in detail above, Scheifler's claim and exemplary embodiments do not limit on the specific locality of the "policy file" (e.g. "centralized policy file" or "central policy file"); Therefore, Scheifler does not limit the security scheme to a centralized scheme.

7. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

8. In response to applicant's arguments with regard to the independent claims 1, 20-21 and 31 rejected under 35 U.S.C. 103(a) that the combination of the references does not teach/suggest the claimed feature "... determining whether the external object has access to other interface of the target object based on the call to the first interface ..." because, in the present invention, access to one interface does not "imply" access to another interface (e.g. Scheifler's disclosure of implied permission does not constitute

Art Unit: 2181

determining access to other interfaces of a target object as the examiner implies); applicant's arguments have fully been considered, but are not found to be persuasive.

The examiner respectfully disagrees; and please note that the features upon which applicant relies (i.e., access to one interface does not "imply" access to another interface) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). And if applicant intends to include the above features into the claims, the examiner requests applicant to cite where in applicant's Specification and/or Drawings support the above features; furthermore, applicant appears to suggest that Scheifler does teach/suggest the above claimed features as applicant indicated that the "... present claims do recite that permissions are implied as described in Scheifler ..." (e.g. interface based access authorization associated with implied permission).

## **I. REJECTIONS BASED ON PRIOR ART**

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2181

9. Claims 1, 4-21 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scheifler et al. (US Patent 6,138,238) in view of Colburn et al. (US Patent 6,173,404).

10. As per claims 1, 20-21 and 31, Scheifler teaches a method, a system and a computer readable storage medium storing instructions for controlling a computer device for controlling access to an object in an operating system, the method, system and computer readable storage medium comprising:

a module configured means for receiving a call from an external thread (Fig. 6, ref. 6200) to a first interface (e.g. write to any file in a directory, such as "c:/") of a target object (Fig. 6, ref. 4500-1) (Fig. 1; Fig. 4-5; col. 4, l. 51 to col. 5, l. 3 and col. 9, l. 11 to col. 14, l. 38);

a module configured with means for determining whether the external thread has access to other interfaces (e.g. write to any specific file in the directory, such as "c:/thisfile") of the target object based on the call received at the first interface (Fig. 4-5 and col. 11, l. 20 to col. 13, l. 45), wherein the determination is in association with implied permission;

wherein the means for determining is solely determined by (based on) the first interface (Fig. 4-5 and col. 11, l. 20 to col. 13, l. 45), as the determination for access to any specific file in a directory (e.g. c:/thisfile) is implied (e.g. solely determined) by the determined accessing to said directory (e.g. c:/); and

a module configured with means for to grant access to the other interfaces according to the determination (Fig. 4-5 and col. 11, l. 20 to col. 13, l. 45).

Scheifler does not expressly teach the method, system and computer readable medium comprising: wherein the call from an object; the target object determining access to the other interfaces; and wherein the determination step comprising means for examining a security policy contained entirely within the target object.

Colburn teaches the method, system and computer readable medium comprising: a call received from an object (Fig. 5, ref. 100); a target object (Fig. 8, ref. 160, 184, 194) determining (at the target object) access to the other interfaces; and wherein the determination step comprising means for examining a security policy (Fig. 8, ref. 184, 194) contained entirely within the target object (Fig. 8, ref. 160) (Fig. 7A-7B; Fig. 8; col. 1, l. 12 to col. 3, l. 45; col. 7, ll. 26-52 and col. 11, l. 25 to col. 12, l. 58), by combination Colburn's target security scheme with Scheifler's permission implementation, the resulting combination further teaches the target object implementing access authorization in association with implied permission to other interfaces, as the target object determines the access authorization of the received call to the other interfaces by examining the target object's own security policies.

It would have been obvious for one of ordinary skill in this art, at the time of invention was made to include Colburn's inter-object security scheme into Scheifler's object for the benefit of implementing a more robust security scheme between objects (Colburn, col. 3, ll. 34-37) to obtain the invention as specified in claims 1, 20-21 and 31.

Art Unit: 2181

11. As per claim 4, Scheifler and Colburn teach all the limitation of claim 1 as discussed above, wherein Scheifler further teaches the method further comprising determining whether the external object and the target object operate in a same process (e.g. same class of valid digital signature or not) (Scheifler, col. 9, l. 52 to col. 11, l. 19).

12. As per claim 5, Scheifler and Colburn teach all the limitation of claim 1 as discussed above, wherein Scheifler further teaches the method comprising wherein determining whether the external object has access to the other interfaces of the target object further comprises: identifying the other interfaces of the target object that can be accessed when the first interface is being requested by the external object (Scheifler, col. 11, l. 20 to col. 13, l. 45), as the other interfaces must be identified in order to proper grant the permission via the implied permission.

13. As per claim 6, Scheifler and Colburn teach all the limitation of claim 1 as discussed above, wherein both further teach the method further comprising determining a first process of the target object (Scheifler, col. 9, l. 52 to col. 11, l. 19 and Colburn, Fig. 8; Fig. 10; col. 1, l. 12 to col. 3, l. 45), such as determining whether the target object's first process corresponds to either valid digital signature with known keys or digital signature that cannot be verified thus a default key is utilized.

14. As per claim 7, Scheifler and Colburn teach all the limitation of claim 6 as discussed above, wherein both further teach the method further comprising determining

Art Unit: 2181

a second process of the external object (Scheifler, col. 9, l. 52 to col. 11, l. 19 and Colburn, Fig. 8; Fig. 10; col. 1, l. 12 to col. 3, l. 45), such as determining whether the external object's second process corresponds to either valid digital signature with known keys or digital signature that cannot be verified thus a default key is utilized.

15. As per claim 8, Scheifler and Colburn teach all the limitation of claim 7 as discussed above, wherein both further teach the method further comprising performing a cross-process communication between the target object and the external object (Scheifler, col. 9, l. 52 to col. 11, l. 19 and Colburn, Fig. 8; Fig. 10; col. 1, l. 12 to col. 3, l. 45; col. 13, l. 44 to col. 14, l. 34), such as allowing restrictive access to the target object as the target object is under valid digital signature process and the external object is not under valid digital signature process.

16. As per claim 9, Scheifler and Colburn teach all the limitation of claim 1 as discussed above, wherein both further teach the method further comprising securing a channel for each interface of the target object (Scheifler, col. 9, l. 52 to col. 11, l. 19 and Colburn, Fig. 8; Fig. 10; col. 1, l. 12 to col. 3, l. 45; col. 13, l. 44 to col. 14, l. 34), as the channel is secured via a cryptographic key over a network between client and server.

17. As per claim 10, Scheifler and Colburn teach all the limitation of claim 1 as discussed above, wherein both further teach the method comprising wherein determining whether the external object has access to the other interfaces of the target

Art Unit: 2181

object further comprises analyzing access constraints within the target object (Scheifler, col. 11, l. 20 to col. 13, l. 45 and Colburn, Fig. 7A-7B; Fig. 8; col. 13, l. 44 to col. 14, l. 34), as the analyzing of the implied permission is located within the target object.

18. As per claim 11, Scheifler and Colburn teach all the limitation of claim 1 as discussed above, wherein both further teach the method further comprising analyzing interface access data stored within the target object (Scheifler, col. 11, l. 20 to col. 13, l. 45 and Colburn, Fig. 7A-7B; Fig. 8; col. 13, l. 44 to col. 14, l. 34).

19. As per claim 12, Scheifler and Colburn teach all the limitation of claim 1 as discussed above, wherein both further teach the method further comprising determining whether the target object and the external object are in a same protection domain (Scheifler, Fig 4; col. 11, l. 20 to col. 13, l. 45 and Colburn, Fig. 8).

20. As per claim 13, Scheifler and Colburn teach all the limitation of claim 12 as discussed above, wherein both further teach the method comprising wherein the protection domain is a process (Scheifler, Fig 4 and col. 9, l. 52 to col. 13, l. 45 and Colburn, Fig. 8), wherein the process is associated with valid digital signature and un-validated digital signature.

21. As per claim 14, Scheifler and Colburn teach all the limitation of claim 1 as discussed above, wherein Colburn further teaches the method comprising wherein the

Art Unit: 2181

target object sets the target object's own security policy (Colburn, Fig. 8), the target object sets the target object's own security policy as the access constraints and access authorization resides within the target object.

22. As per claim 15, Scheifler and Colburn teach all the limitation of claim 1 as discussed above, wherein Scheifler further teaches the method comprising wherein determining whether the external object has access to the other interfaces further comprises determining capabilities of the external object (Scheifler, col. 9, l. 52 to col. 13, l. 45), as the capability corresponds to the capability of transferring data along with the know key or without the know key.

23. As per claim 16, Scheifler and Colburn teach all the limitation of claim 15 as discussed above, wherein Colburn further teaches the method comprising further comprising mapping capabilities of the external object to the other interfaces of the target object (Scheifler, col. 9, l. 52 to col. 13, l. 45), such as mapping the capability of transferring data with the know key to other interfaces for grater access.

24. As per claim 17, Scheifler and Colburn teach all the limitation of claim 1 as discussed above, wherein both further teach the method comprising wherein the target object and the external object are created using a same methodology (e.g. object oriented by Java) (Scheifler, col. 9, l. 52 to col. col. 11, l. 19 and Colburn, col. 1, l. 12 to col. 3, l. 45).

25. As per claim 18, Scheifler and Colburn teach all the limitation of claim 1 as discussed above, wherein Colburn further teaches the method comprising wherein the target object and the external object are views in a view hierarchy (Colburn, col. 1, l. 12 to col. 3, l. 45).

26. As per claim 19, Scheifler and Colburn teach all the limitation of claim 18 as discussed above, wherein Colburn further teaches the method comprising wherein a view has a parent calling interface, a child calling interface, and a child managing interface (Colburn, col. 6, ll. 29-52), as the hierarchal relation between parent-child is well known with the corresponding above interfaces for the parent and the child.

## **II. CLOSING COMMENTS**

### **Conclusion**

#### **a. STATUS OF CLAIMS IN THE APPLICATION**

The following is a summary of the treatment and status of all claims in the application as recommended by **M.P.E.P. 707.07(i)**:

##### **a(1) CLAIMS REJECTED IN THE APPLICATION**

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

#### **b. DIRECTION OF FUTURE CORRESPONDENCES**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chun-Kuan (Mike) Lee whose telephone number is (571) 272-0671. The examiner can normally be reached on 8AM to 5PM.

### **IMPORTANT NOTE**

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Alford Kindred can be reached on (571) 272-4037. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Chun-Kuan Lee/  
Primary Examiner  
Art Unit 2181  
April 03, 2012